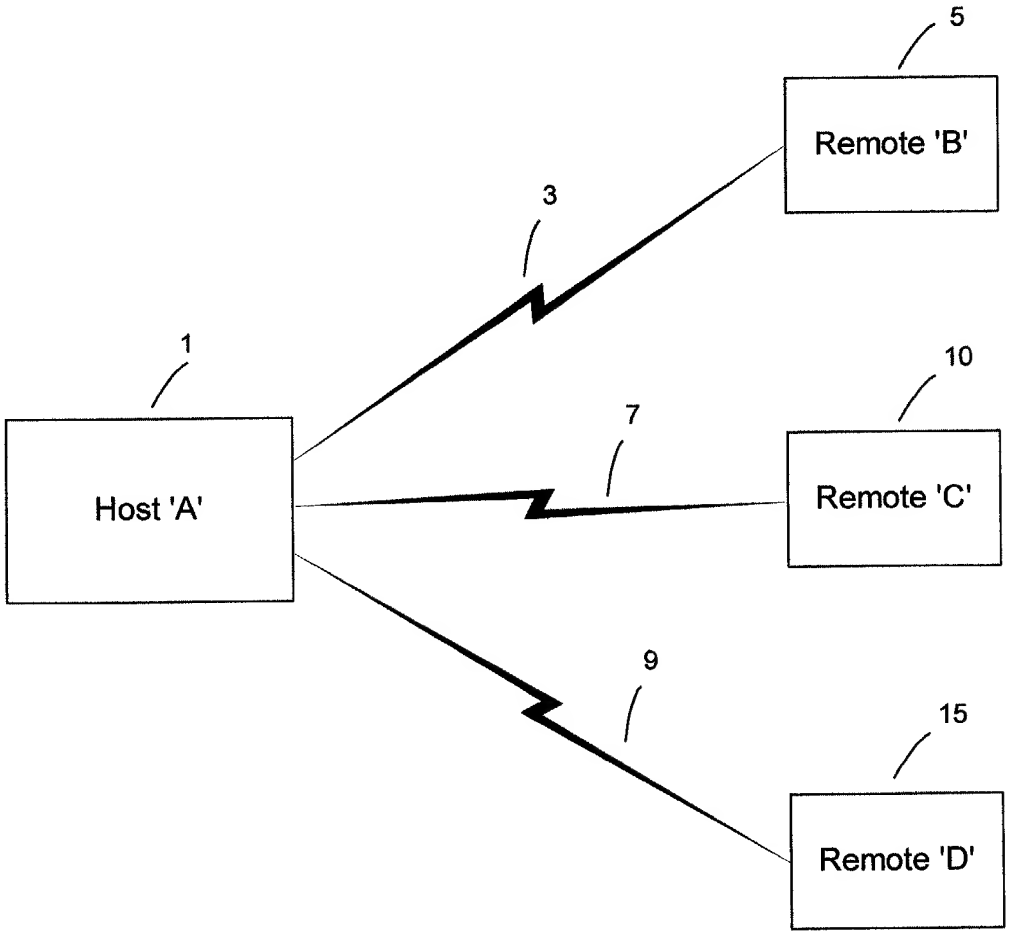

FIG. 1

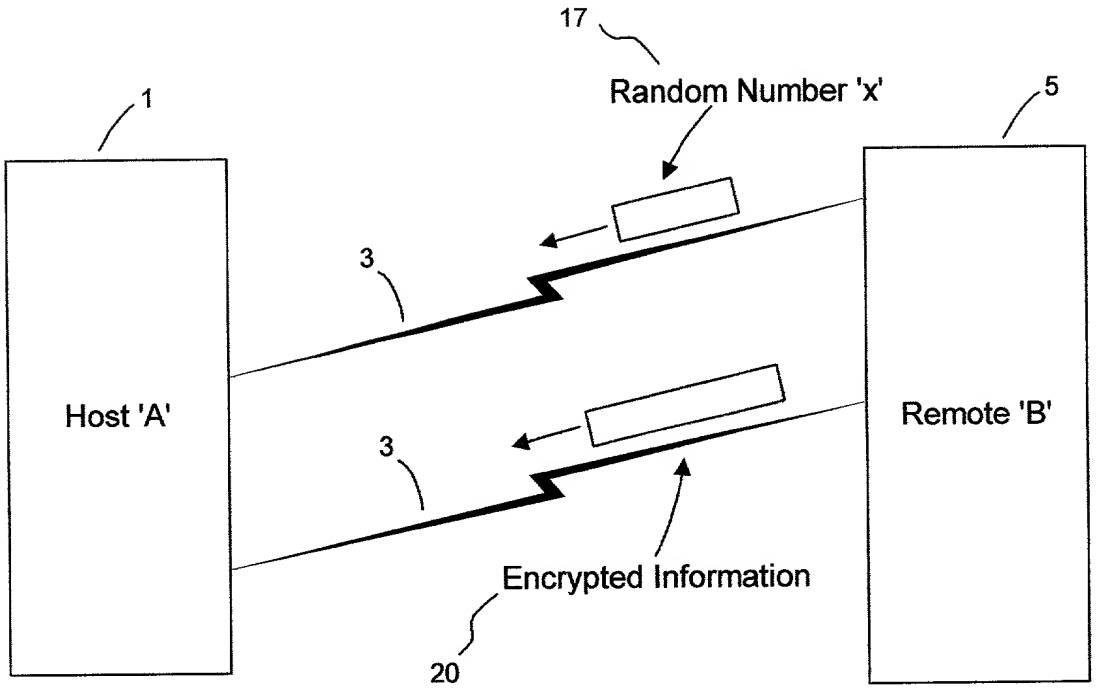
17
Random Number 'x'
1
5
3
Host 'A'
Remote 'B'
3
Encrypted Information
20

FIG. 2

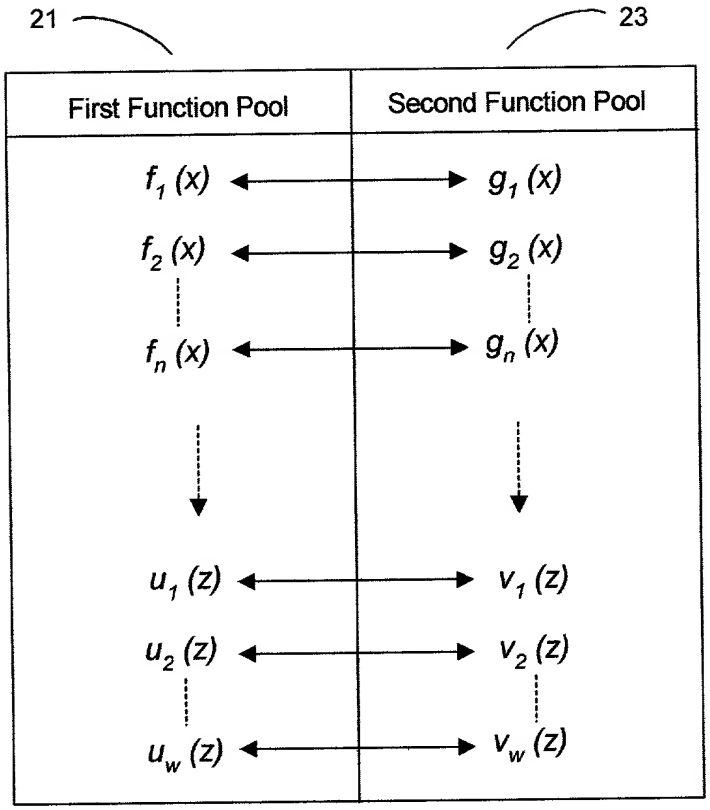
21
23
First Function Pool
Second Function Pool
$f_1(x)$
$g_1(x)$
$f_2(x)$
$g_2(x)$
$f_n(x)$
$g_n(x)$
$u_1(z)$
$v_1(z)$
$u_2(z)$
$v_2(z)$
$u_w(z)$
$v_w(z)$

FIG. 3

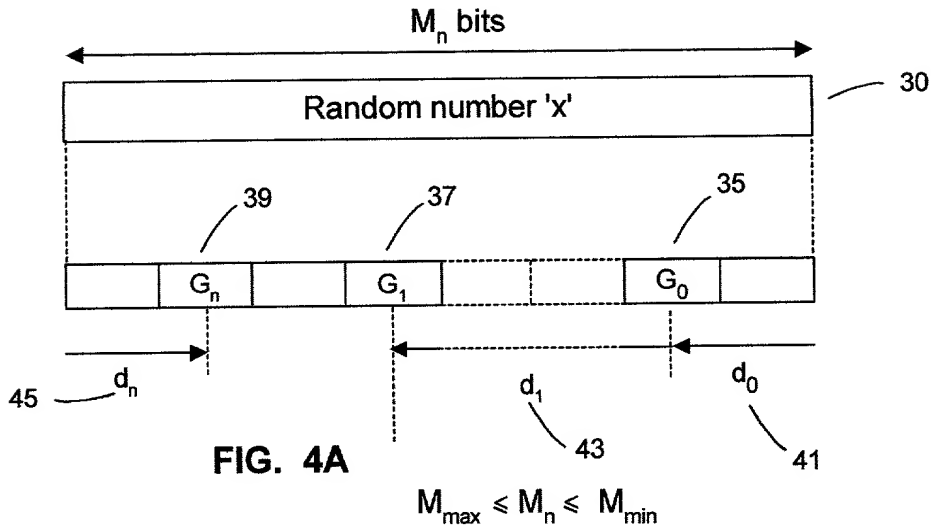

FIG. 4A

$M_{max} \leq M_n \leq M_{min}$

Table for M_n

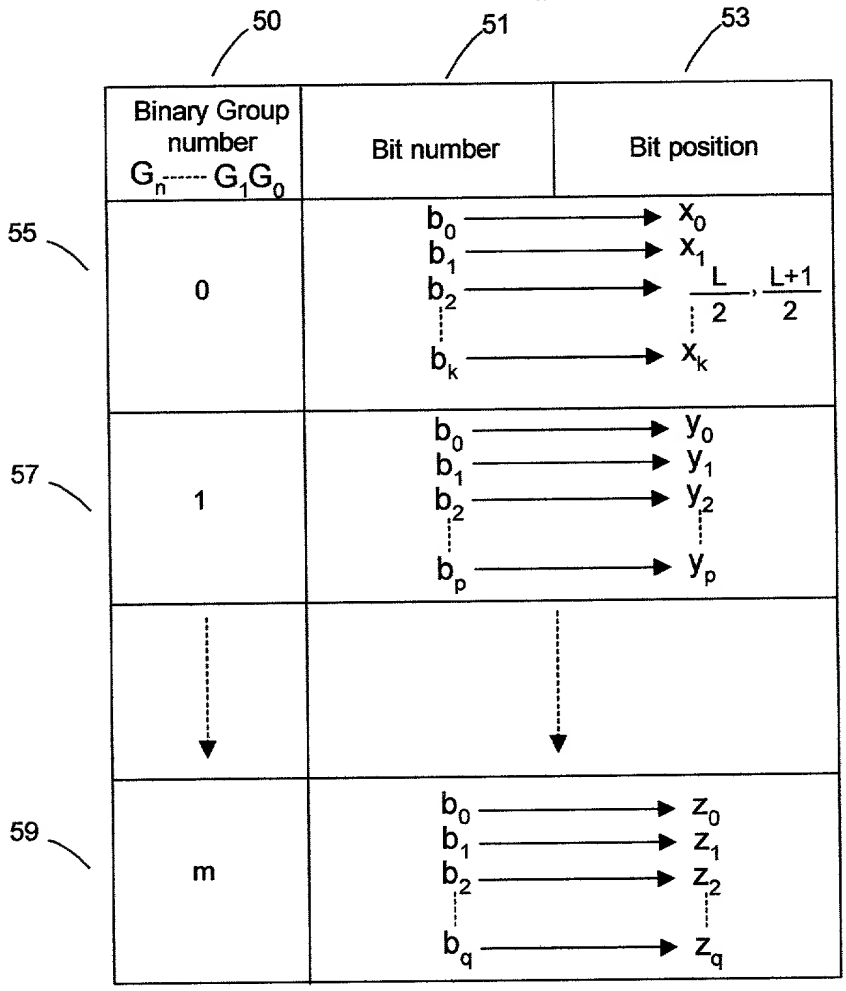

FIG. 4B

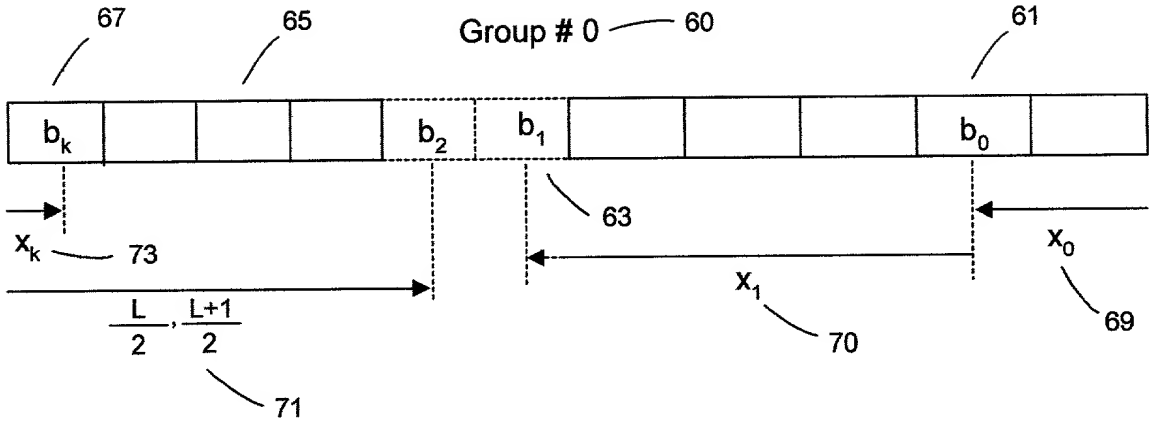

FIG. 5A

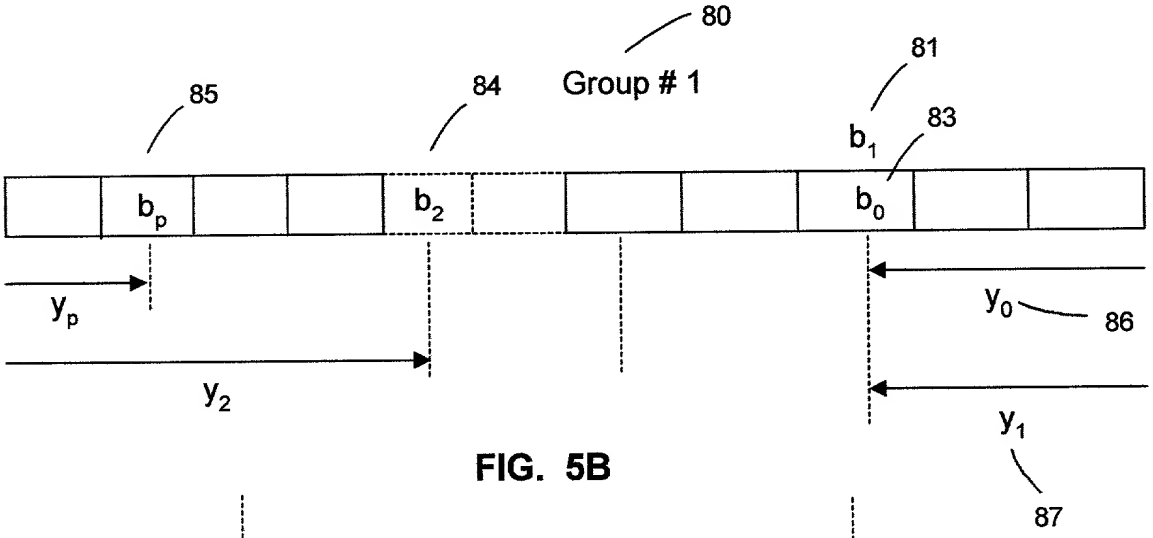

FIG. 5B

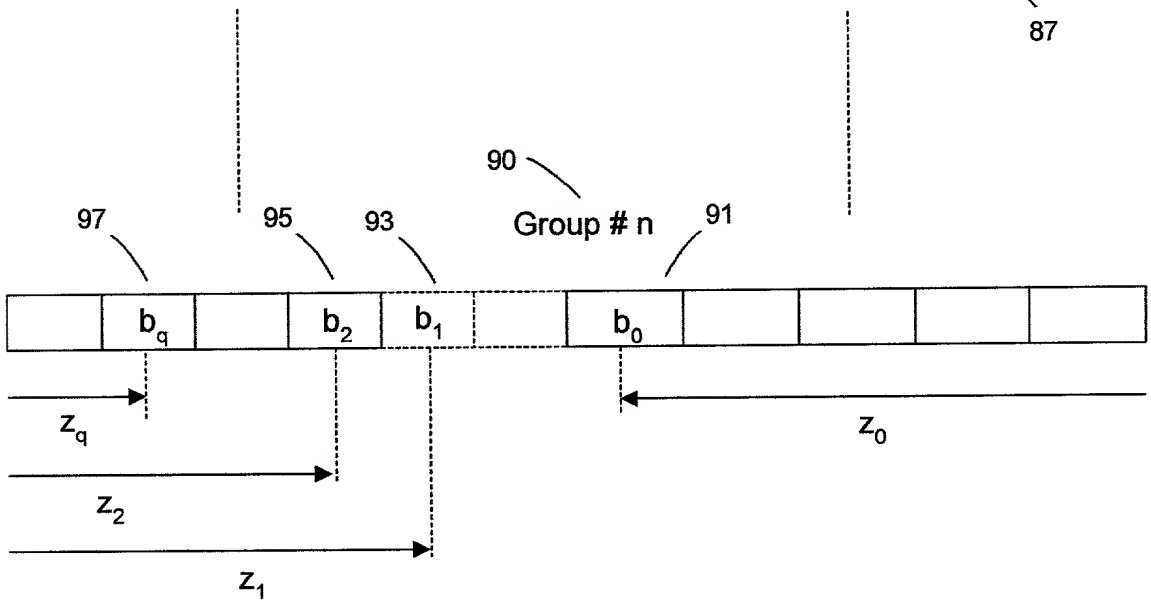

FIG. 5C

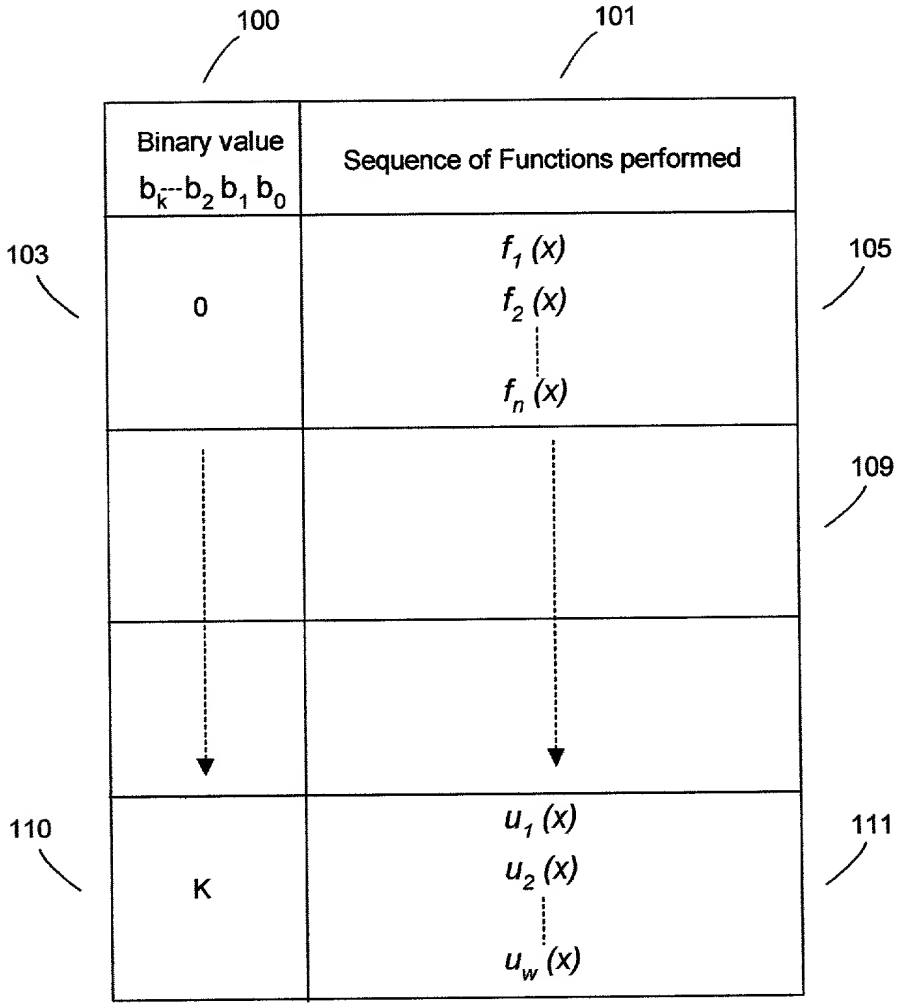
100
101
Binary value
b_k---b_2 b_1 b_0
Sequence of Functions performed
103
105
0
$f_1(x)$
$f_2(x)$
$f_n(x)$
109
110
111
K
$u_1(x)$
$u_2(x)$
$u_w(x)$

FIG. 6

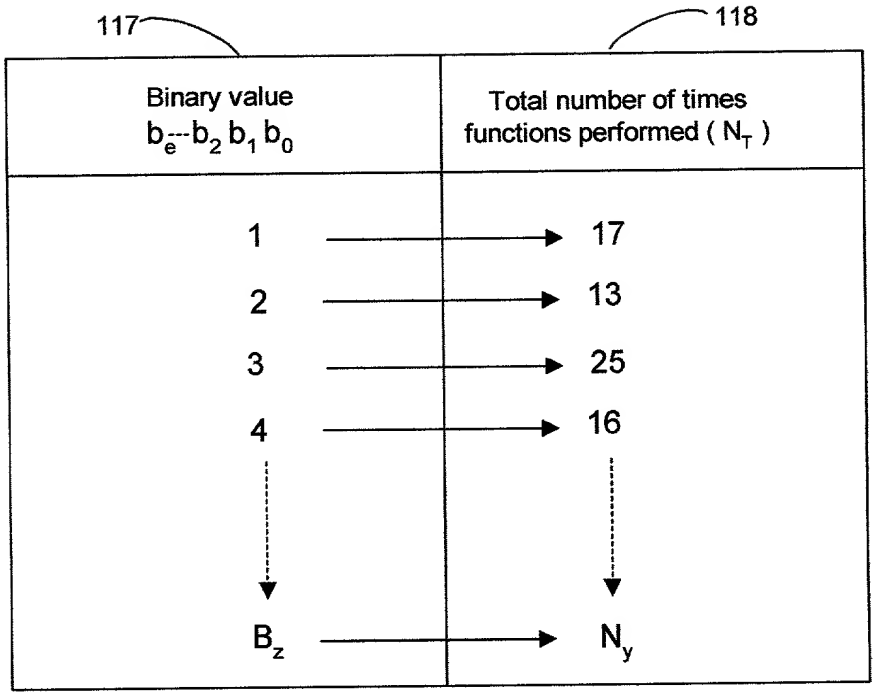
117
118
Binary value
b_e---b_2 b_1 b_0
Total number of times functions performed (N_T)
1
2
3
4
B_z
17
13
25
16
N_y

FIG. 7

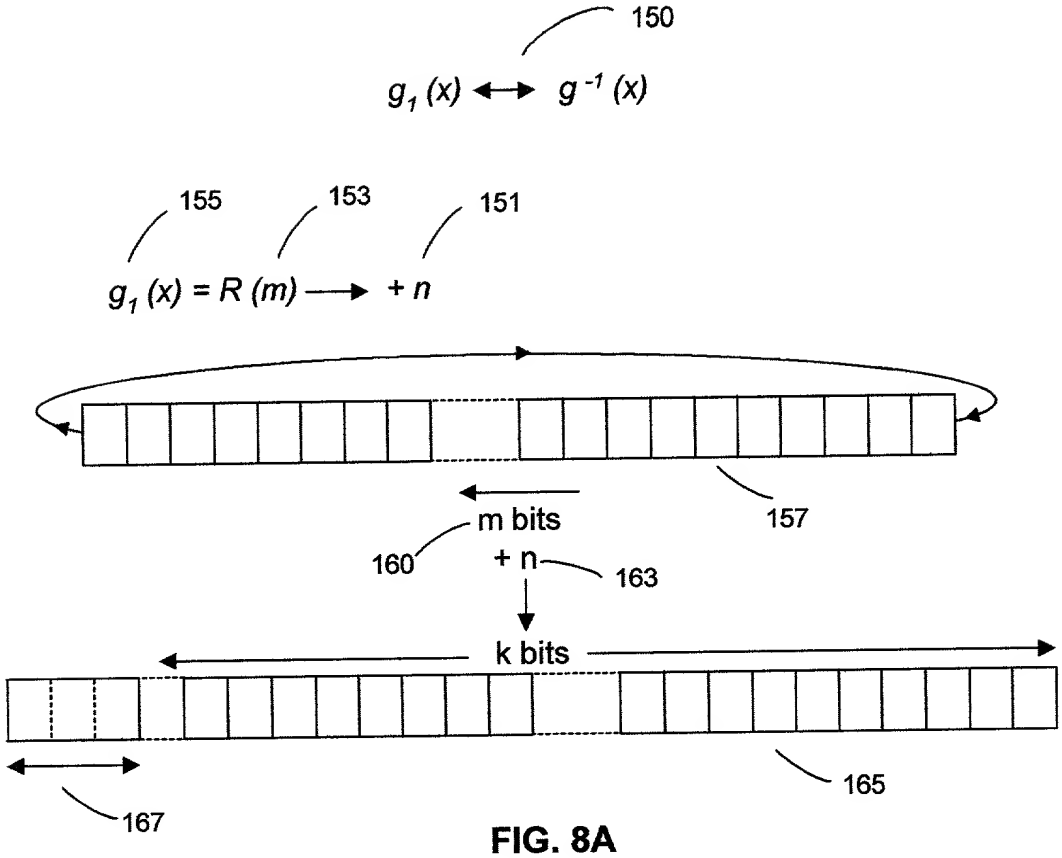
150
$g_1(x) \longleftrightarrow g^{-1}(x)$
155
153
151
$g_1(x) = R(m) \longrightarrow +n$
m bits
157
160
+ n
163
k bits
165
167

FIG. 8A

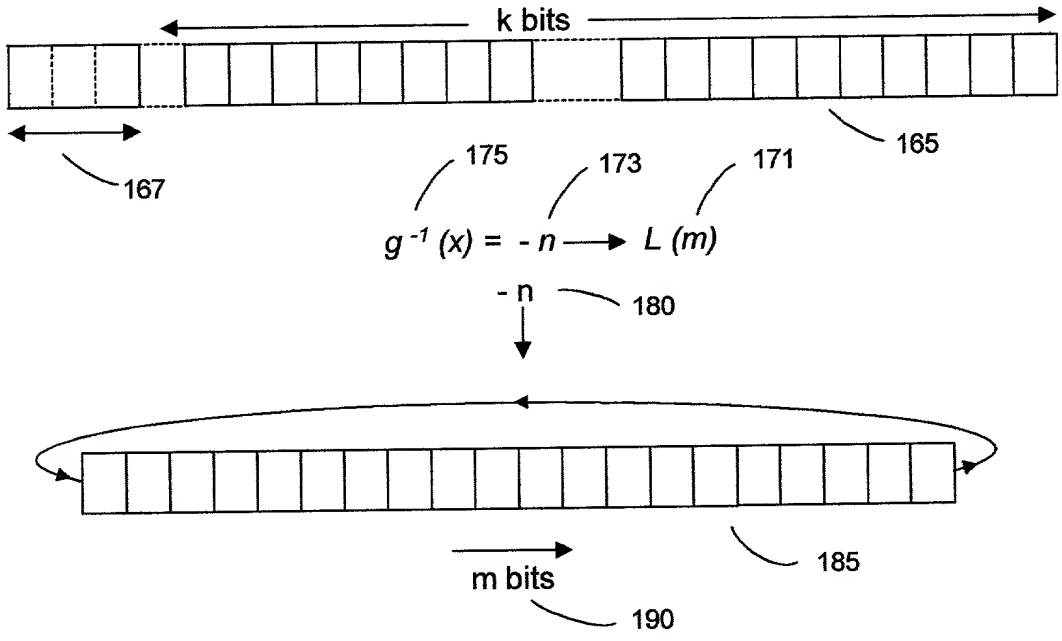
k bits
165
167
175
173
171
$g^{-1}(x) = -n \longrightarrow L(m)$
- n
180
185
m bits
190

FIG. 8B

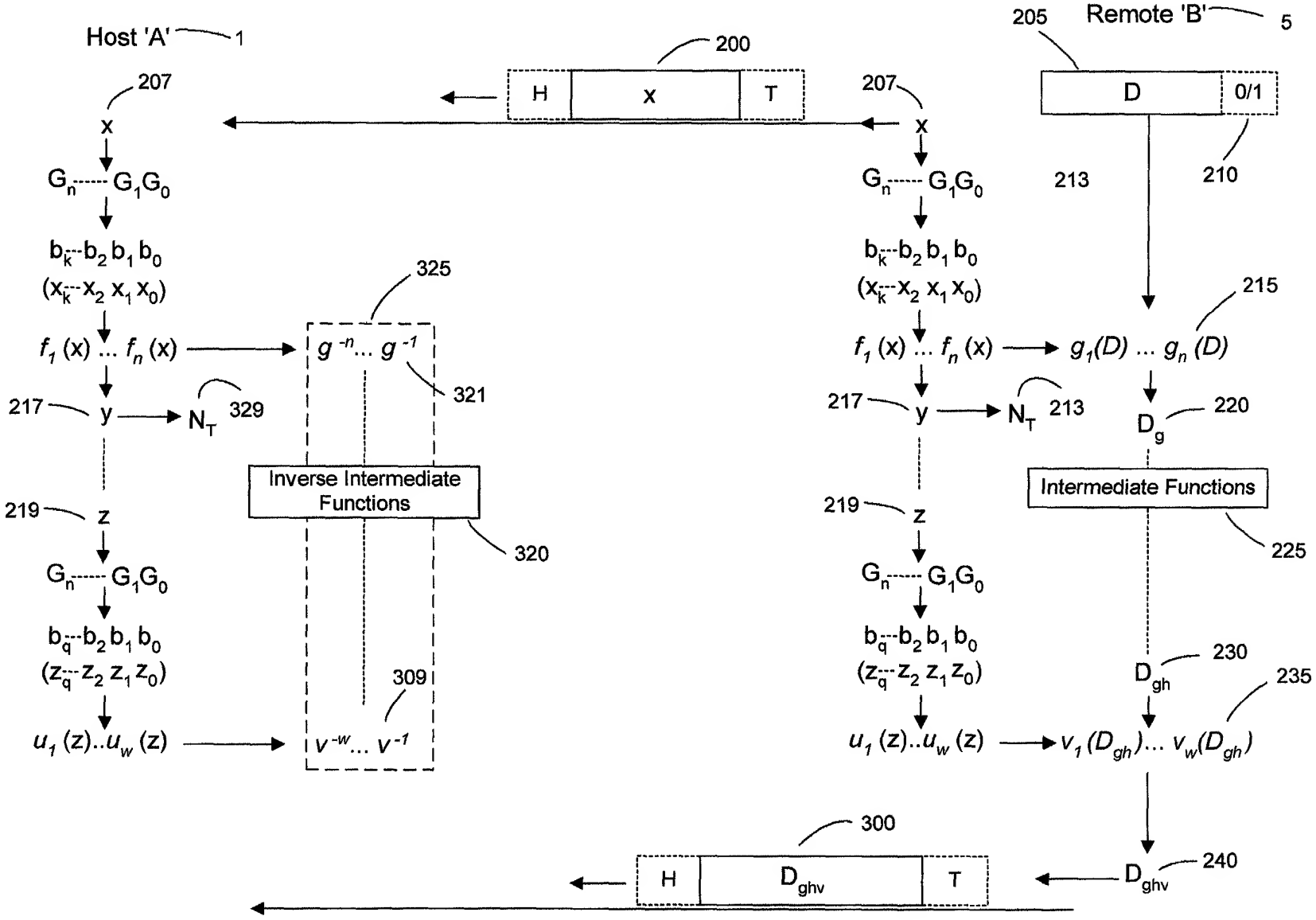
Host 'A'
1
Remote 'B'
5
205
200
H
x
T
D
0/1
207
207
213
210
$G_n \cdots G_1 G_0$
$b_k \cdots b_2 b_1 b_0$
$(x_k \cdots x_2 x_1 x_0)$
$f_1(x) \ldots f_n(x)$
$g_1(D) \ldots g_n(D)$
215
325
$g^{-n} \ldots g^{-1}$
321
217
y
N_T
329
213
220
D_g
Inverse Intermediate Functions
Intermediate Functions
219
z
320
225
$b_q \cdots b_2 b_1 b_0$
$(z_q \cdots z_2 z_1 z_0)$
230
D_{gh}
235
309
$u_1(z) .. u_w(z)$
$v^{-w} \ldots v^{-1}$
$v_1(D_{gh}) \ldots v_w(D_{gh})$
300
H
D_{ghv}
T
240

FIG. 9

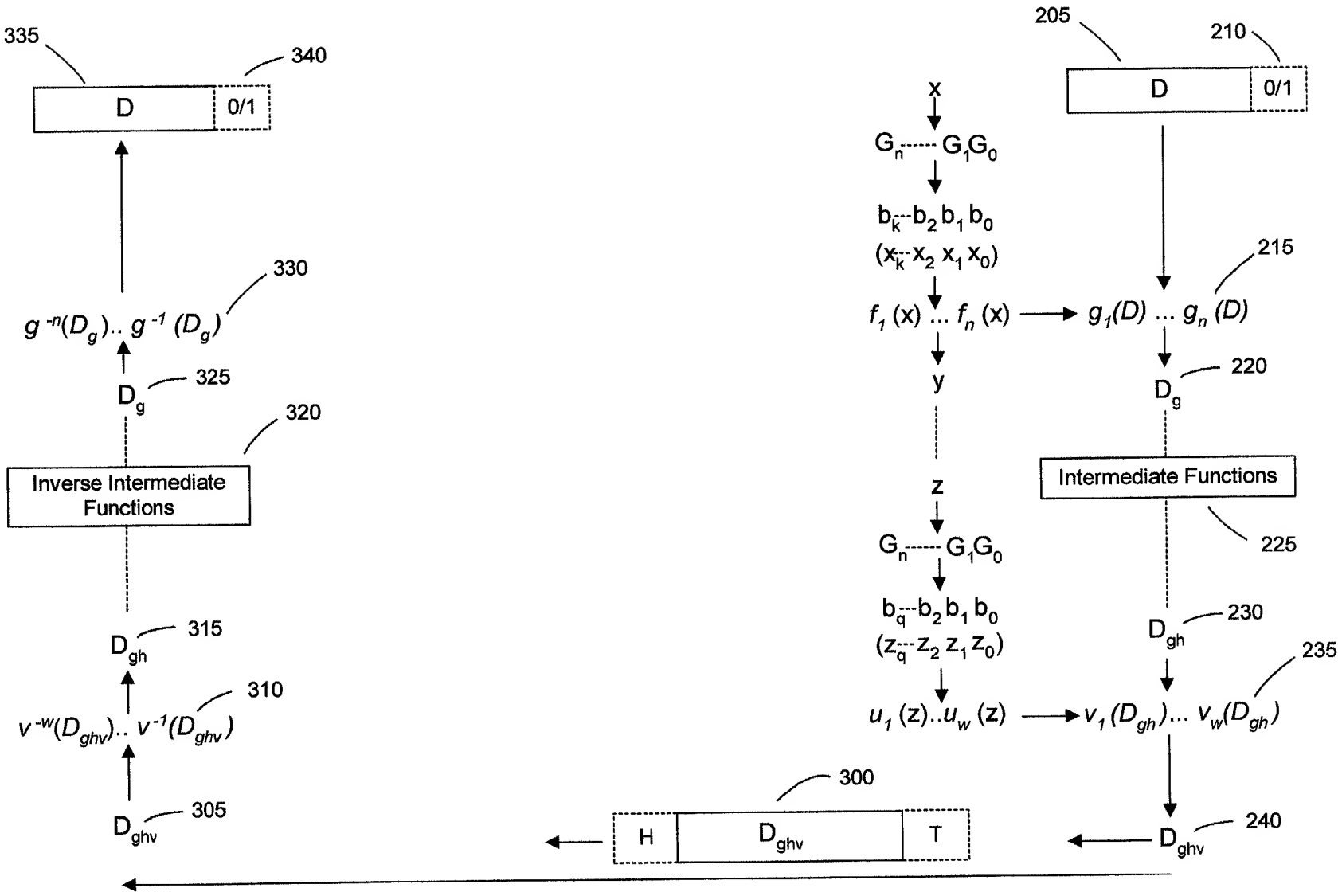
335
340
D
0/1
330
$g^{-n}(D_g)..\ g^{-1}(D_g)$
325
D_g
320
Inverse Intermediate Functions
315
D_{gh}
310
$v^{-w}(D_{ghv})..\ v^{-1}(D_{ghv})$
305
D_{ghv}
205
210
D
0/1
x
G_n ---- G_1G_0
b_k --- $b_2\ b_1\ b_0$
(x_k --- $x_2\ x_1\ x_0$)
$f_1(x)$ ... $f_n(x)$
215
$g_1(D)$ ... $g_n(D)$
y
220
D_g
Intermediate Functions
z
225
G_n ---- G_1G_0
b_q --- $b_2\ b_1\ b_0$
(z_q --- $z_2\ z_1\ z_0$)
230
D_{gh}
235
$u_1(z)..u_w(z)$
$v_1(D_{gh})$... $v_w(D_{gh})$
300
H
D_{ghv}
T
240
D_{ghv}

FIG. 10

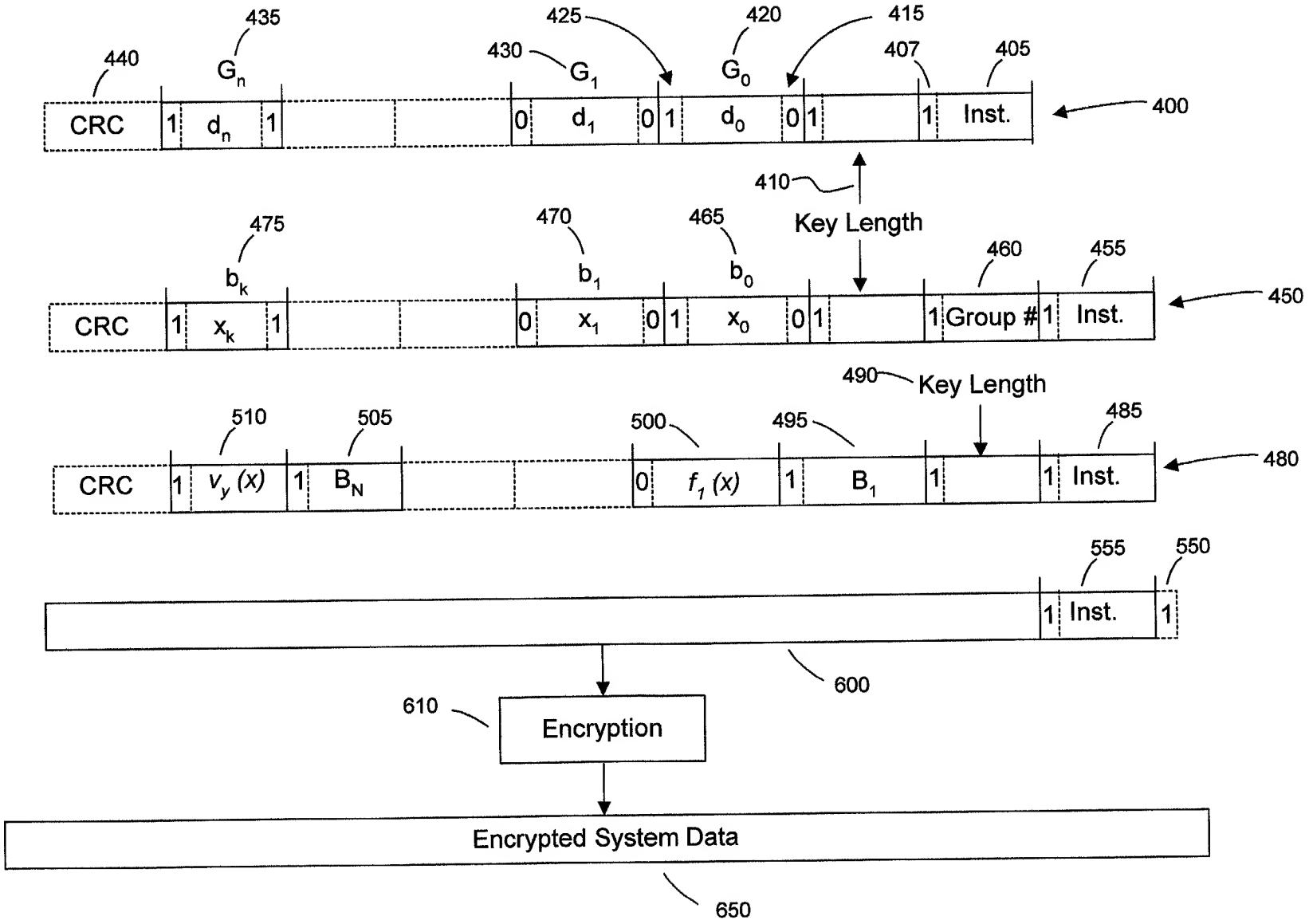
435
425
420
415
440
G_n
430
G_1
G_0
407
405
CRC
1
d_n
1
0
d_1
0
1
d_0
0
1
1
Inst.
400
410
Key Length
475
470
465
460
455
b_k
b_1
b_0
CRC
1
x_k
1
0
x_1
0
1
x_0
0
1
1
Group #
1
Inst.
450
490
Key Length
510
505
500
495
485
CRC
1
v_y (x)
1
B_N
0
f_1 (x)
1
B_1
1
1
Inst.
480
555
550
1
Inst.
1
600
610
Encryption
Encrypted System Data
650

FIG. 11

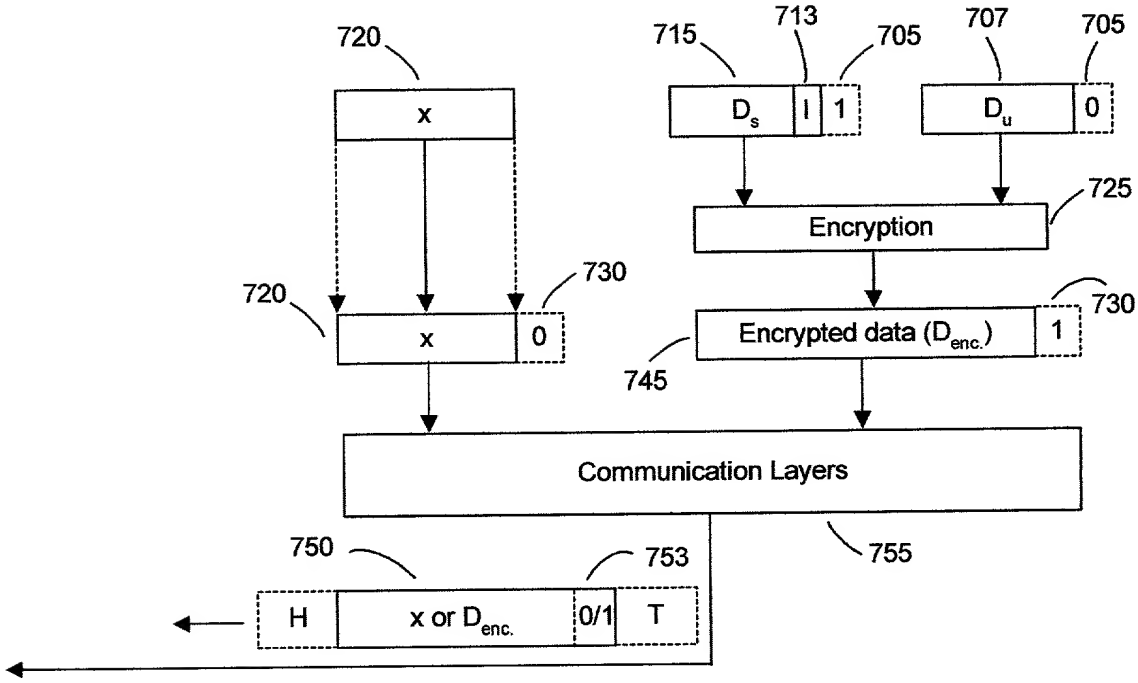

FIG. 12A

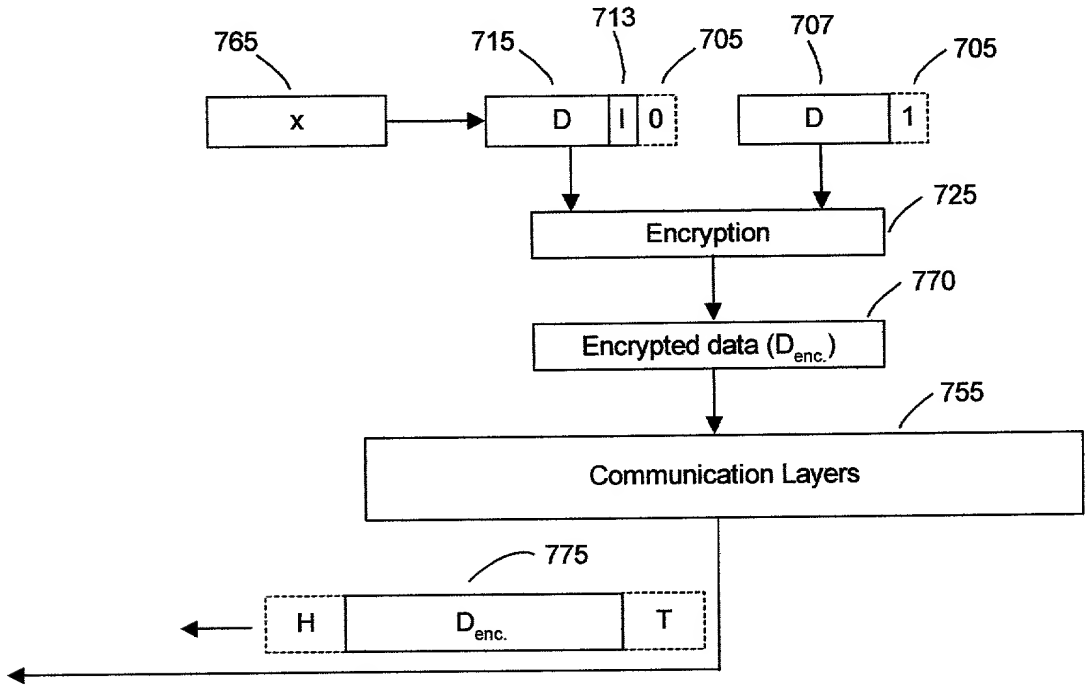

FIG. 12B

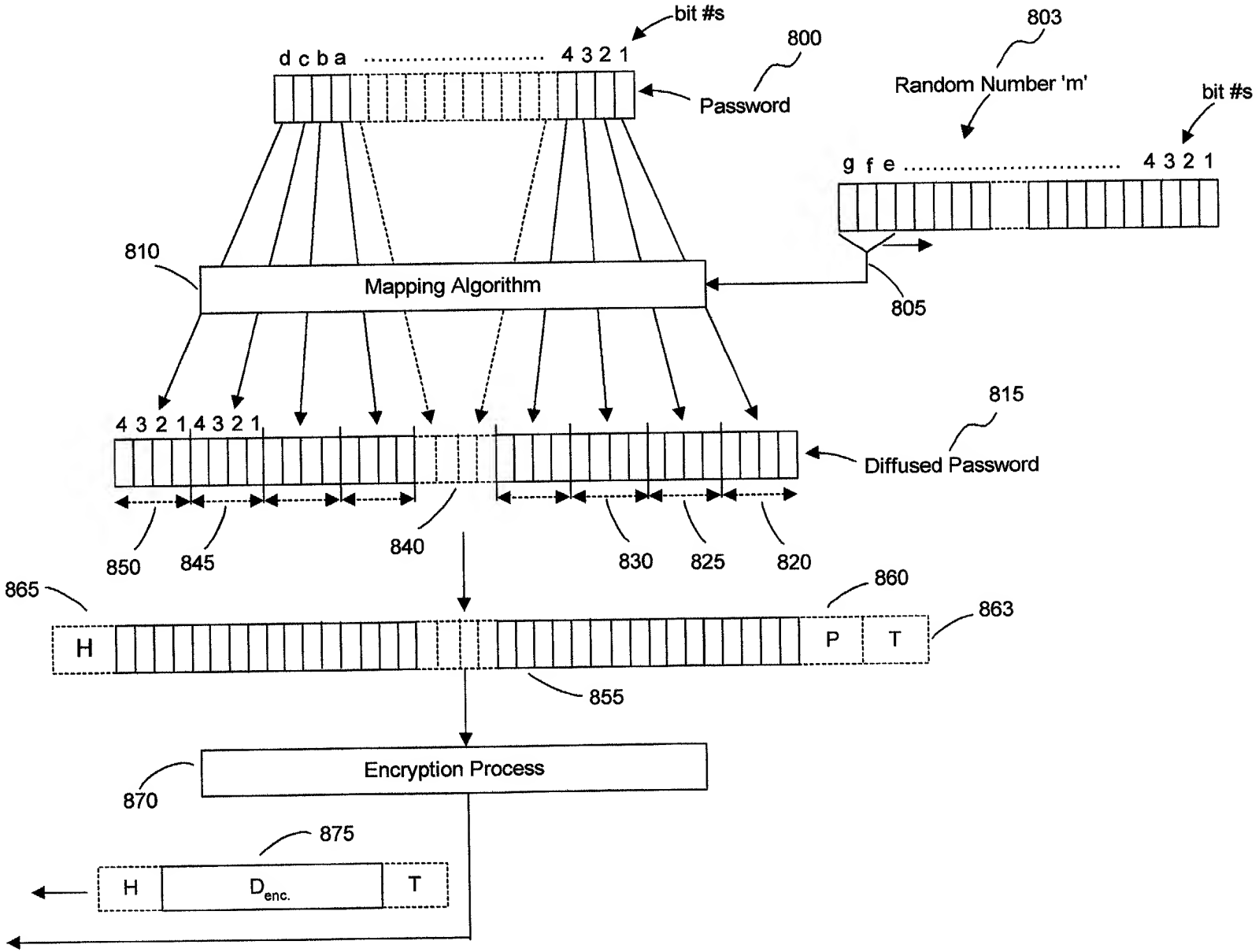
bit #s
d c b a 4 3 2 1
800
Password
803
Random Number 'm'
bit #s
g f e 4 3 2 1
810
Mapping Algorithm
805
4 3 2 1 4 3 2 1
815
Diffused Password
850
845
840
830
825
820
865
860
863
H
P
T
855
Encryption Process
870
875
H
$D_{enc.}$
T

FIG. 13

Table for Mapping Algorithm

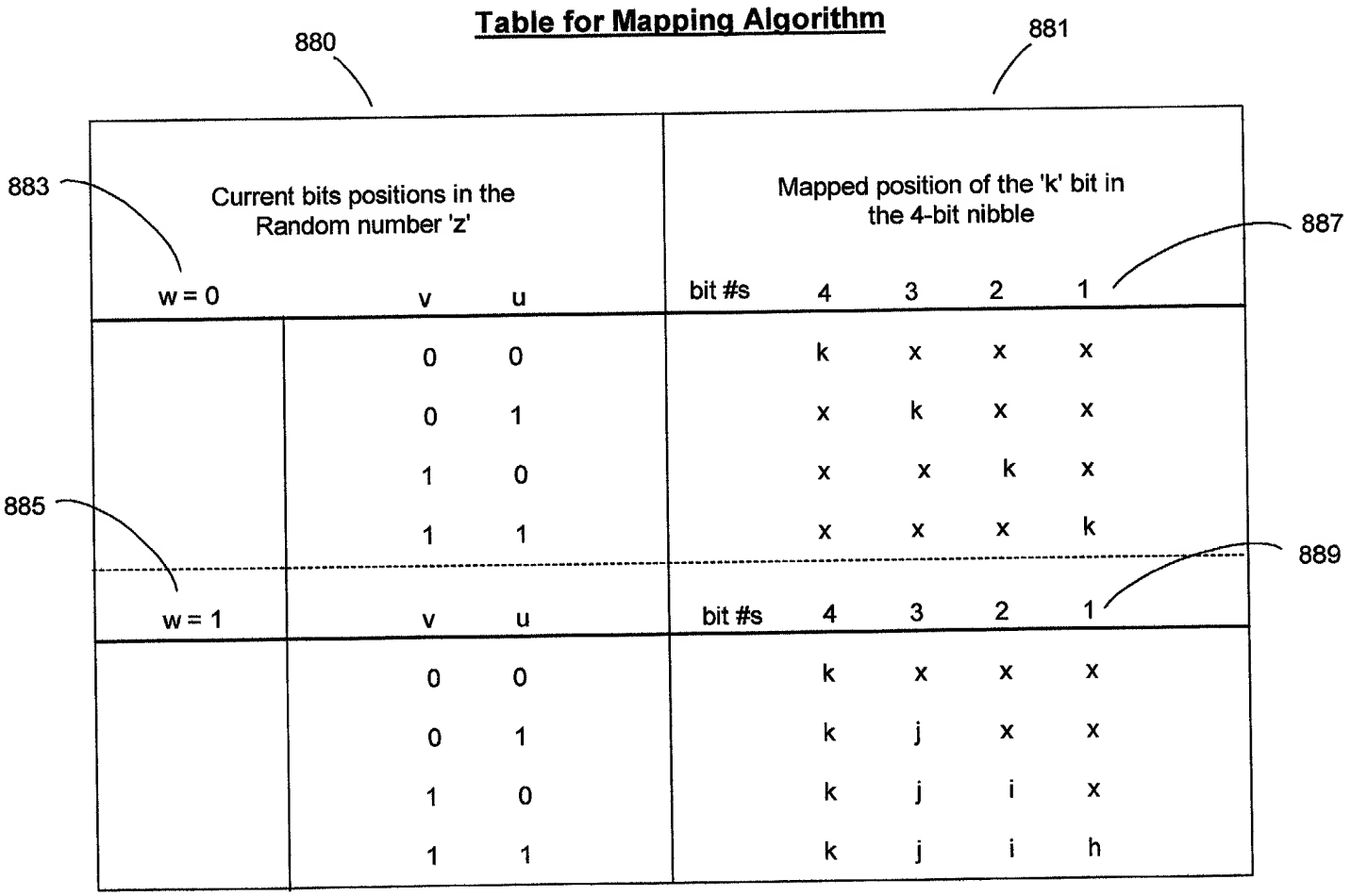

FIG. 14